



Top Questions on AI Regulation

REVERA
25+ years of legal experience

1. Is content created by artificial intelligence (AI) protected by copyright?

Copyright for a work (such as creative works, designs, source code, or videos) arises when there is a human creative contribution. If there is no such contribution — for example, if AI generates art based on a one-sentence prompt — this art is not protected by copyright.

If a work is created with the help of AI, copyright protection is possible if the author made significant efforts in its creation, for example, in the following cases:

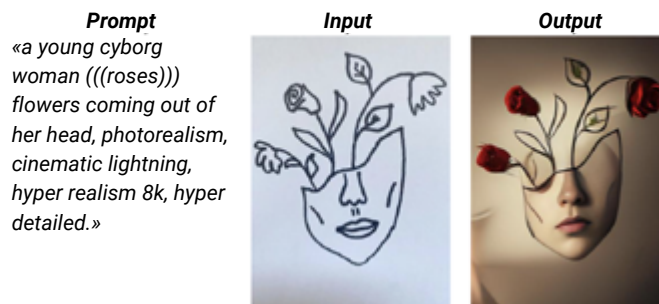
- ✦ The author provided original input, such as hand-created art that AI refined.
- ✦ The author created the work using AI after a long series of prompts.
- ✦ The author created the work using AI and made significant manual adjustments.
- ✦ The author created several works using AI and compiled them into a larger work, such as a clip or a film made up of smaller segments generated by AI.

For the latter example, an established precedent is the position of the US Copyright Office, which is well-known for the case involving Christina Kashanova's comics, which — in the view of the Copyright Office — do not possess sufficient creative character because they were generated by AI. However, the work is protected as a compilation, as it was created through Ms Kashanova's creative effort: the selection and arrangement of images, as well as the accompanying text.



Another example of partial protection:

The AI system produced this output:



The Copyright Office allowed registration with the note “Registration limited to unaltered human pictorial authorship []”, meaning the drawing and text, but not the final 3D output.

Approaches to AI content protection vary by jurisdiction and are evolving rapidly. It is therefore essential to regularly monitor legal positions in key markets and document the entire creation process, from initial prompts to final edits. It is recommended to implement an AI Policy for your team and contractors, outlining the rules for AI usage and documentation requirements — this will form the basis for protecting your copyrights.

2. Who owns the copyright for AI-created content?

If AI content is protected by copyright, as described in Question 1, the author is usually recognised as the person who created the content through their creative effort. Society has not yet fully embraced the idea of co-authorship with AI.

Thus, the rights to the output may belong to the developers of the AI systems or their users. Today, this issue is typically addressed through user agreements.

The owner of a GenAI platform is generally not considered the owner of the rights to the content generated using their platform, with user relationships governed by Terms of Use. In most AI products, such as ChatGPT, Midjourney, etc., the rights to the output are attributed to the users.

3. Can AI models be trained on protected materials?

In some countries, exceptions allow AI to be trained on publicly available content unless there is a direct prohibition by the data owner. For example, in the EU, there is the Text & Data Mining exception, which is relied upon by most GenAI models. However, the data owner can prohibit the use of their information, for example, by placing a robots.txt file on their website, which automatically prevents AI from analysing the data.

However, the situation does not have a clear-cut answer, particularly concerning the boundaries of this exception and in which cases it allows data to be used. Furthermore, most large platforms have specified in their policies that their data cannot be used for AI training.

With the growing number of cases like OpenAI v. The New York Times and UMG Recordings v. Suno, where works are integrated into original projects (e.g., preparing website designs or game characters), we recommend obtaining a licence.

4. Is it legal to use personal data of employees and job applicants when using AI?

There is no direct prohibition, but strict GDPR limitations and increasing litigation risks apply. Using AI in HR is not banned, but you must comply with all GDPR requirements for processing personal data. This means:

- ✦ Mandatory notification of candidates and employees that their data is being processed by AI systems,
- ✦ Timely deletion of data after the recruitment process ends,
- ✦ Strictly prohibiting the use of special categories of data (e.g., race, religion, political views) without explicit consent.

The use of AI screening tools is under question; in the case of *Mobley v. Workday*, plaintiffs argue that algorithms discriminate against candidates over 40 years old. The ruling in this case will set an important precedent for the industry.

In the context of screening tools, remember the ban on automated decision-making. GDPR prohibits decisions regarding hiring, firing, or promotion solely based on automated processing.

This means you cannot simply rely on an AI agent to make decisions; there must always be human review of each decision.

When implementing AI in HR, conduct a DPIA (Data Protection Impact Assessment). This is a mandatory requirement for high-risk systems. A DPIA will help identify and mitigate discrimination risks and will serve as your protection in case of regulatory scrutiny.

5. Who is responsible for AI errors?

As a general rule, the entity or organisation providing the end service using AI is liable for errors related to AI usage. For example, if Company X's IT system generates predictions based on fingerprint data and is integrated with an AI API (such as ChatGPT), Company X is generally responsible for the accuracy and results of this system towards the user, not OpenAI.

However, according to the EU AI Act, AI system providers (including high-risk systems) may be held liable for non-compliance with AI system quality requirements.

6. What are the legal requirements for using AI in game development?

Using AI in games is governed by general legal norms but with significant industry-specific features.

AI-generated content in games is subject to standard copyright, data protection, and content liability requirements. Platforms set their own rules for AI content. Steam requires developers to guarantee the legality of AI-generated content, its compliance with marketing materials, and the implementation of mechanisms to prevent the creation of illegal content in real time. Moreover, in Adult Only games, real-time AI content generation is completely prohibited. Epic Games, PlayStation, and Xbox also have their own policies, which need to be reviewed separately for each platform.

Practical recommendations:

- ✦ Mark AI-generated content and document processes,
- ✦ Always indicate in the game description the use of AI to generate content,
- ✦ Keep documentation on the sources of training data,
- ✦ Implement moderation systems for real-time content generation.

Pay particular attention to protecting data of underage players, as this is an area of heightened regulatory scrutiny.

7. What risks are associated with using AI-generated content?

Intellectual property risks: The main threat is lawsuits from copyright holders for using their materials in training datasets without permission. A recent example is the ruling in the case *Thomson Reuters v. ROSS Intelligence (2025)*, which established that training AI on copyright-protected materials could constitute a direct infringement. Additional risks include the lack of copyright for AI-generated content, making your developments vulnerable to being copied by competitors.

Service quality and operational disruptions: AI systems may produce inaccurate results, hallucinations, or discriminatory decisions, leading to customer dissatisfaction and reputational damage. This is particularly critical for customer service bots, medical applications, and financial services. AI system technical failures could paralyse business processes if no backup systems are in place.

GDPR risks and data breaches: AI usage often involves processing large volumes of personal data without a clear legal basis, which is a direct violation of GDPR, with fines up to €20 million. AI systems also create new attack vectors: model inversion attacks can extract training data, and prompt injection can access internal company information.

Regulatory risks of a new generation: The EU AI Act introduces fines up to €35 million for non-compliance with high-risk AI system requirements. In the US, state-level industry regulations are increasing. Companies risk finding themselves in a situation where their AI systems suddenly fall under new requirements that cannot be met without radically overhauling their architecture.

8. Can AI agents be used for sales and communication with clients?

Technically, yes, but with mandatory disclosure of AI usage.

In most jurisdictions, there is no direct prohibition on using AI agents for sales, but there is a requirement for honesty in commercial relationships. Clients must understand they are interacting with AI, not a human. The EU AI Act mandates clear labelling of AI-generated content, and consumer protection laws in many countries prohibit misleading commercial practices.

Personal data processing requires special attention. The AI agent will process clients' personal data (names, contacts, preferences), automatically making you subject to GDPR. You must update your privacy policy to include the use of AI for data processing, ensure data deletion on client request, and limit AI access to only the necessary information. It is especially important not to train AI on clients' confidential data without their consent.

Set clear boundaries for authority and quality control. Determine what decisions the AI can make independently (e.g., scheduling meetings) and which require human involvement (e.g., signing contracts, granting discounts). Implement a system to monitor AI interactions and an escalation procedure for complex cases.

Remember: your company is legally responsible for the actions of the AI agent, so any promises or agreements made by AI could become legally binding.

9. How to legally protect myself if I want to create an AI model (agent, assistant), train it, and launch it as an independent product or part of an IT product?

It's difficult to completely eliminate risks when using AI systems in this way. Based on the risks described above and our experience, we recommend, at a minimum, adhering to the following rules:

- ✦ Enter into agreements with employees and contractors that outline the rules for using and developing AI systems and working with open-source databases (limitations on copyleft licences, mandatory reporting, etc.),
- ✦ Develop internal policies for working with AI and open-source datasets,
- ✦ Develop and publish an EULA (End-User Licence Agreement) and distribute risks with users depending on the jurisdiction of the business,
- ✦ Hire a DPO (Data Protection Officer) for auditing compliance with personal data regulations,
- ✦ Conduct intermediate legal audits to check the "cleanliness" of rights to IT products and compliance with regulatory requirements in the AI field.

And remember, AI is not only a powerful tool for business development but also a significant legal challenge for those building transparent businesses with long-term prospects.

For more detailed information on launching an AI-powered startup, read our specialised guide.

If you have other questions related to AI, the REVERA team is ready to assist you!

